

Requested Patent: FR2819322A1

Title:

METHOD FOR ASSESSING AND MANAGING SECURITY OF COMPUTER SYSTEM
OF CERTAIN CONFIGURATION BY PERFORMING COMPARATIVE ANALYSIS
BETWEEN FIRST AND SECOND DATABASES TO ASSESS POSSIBLE
PROBLEMS THAT MIGHT AFFECT COMPUTER SYSTEM ;

Abstracted Patent: FR2819322 ;

Publication Date: 2002-07-12 ;

Inventor(s):

BUR GUILLAUME; PONS BENOIT; BEHAR MARC; BIDOU RENAUD; SADIRAC
NICOLAS ;

Applicant(s): VERISEC (FR) ;

Application Number: FR20010000192 20010108 ;

Priority Number(s): FR20010000192 20010108 ;

IPC Classification: G06F12/14; G06F17/60 ;

Equivalents: ;

ABSTRACT:

The computer system may be sensitive to one or several problems. From a first database (30) a configuration of the computer system is retrieved. A second database (80) may store a number of known security threads. Comparative analysis (40), between the first and second databases (30,80) is performed in order to assess the possible problems that might affect the computer system. An Independent claim is included for a device for evaluation a security level

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①1 N° de publication :

2 819 322

(à n'utiliser que pour les
commandes de reproduction)

②1 N° d'enregistrement national :

01 00192

⑤1 Int Cl⁷ : G 06 F 12/14, G 06 F 17/60

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 08.01.01.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 12.07.02 Bulletin 02/28.

⑤6 Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule*

⑥0 Références à d'autres documents nationaux
apparentés :

⑦1 Demandeur(s) : VERISEC Société anonyme — FR.

⑦2 Inventeur(s) : SADIRAC NICOLAS, BIDOU
RENAUD, BEHAR MARC, BUR GUILLAUME et PONS
BENOIT.

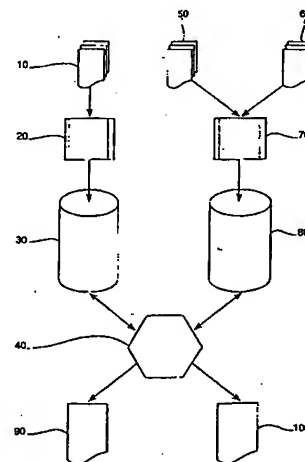
⑦3 Titulaire(s) :

⑦4 Mandataire(s) : CABINET WAGRET.

⑤4 PROCÉDE ET DISPOSITIF D'ÉVALUATION DE LA SÉCURITÉ D'UN SYSTÈME INFORMATIQUE.

⑤7 La présente invention concerne un procédé d'évaluation et de gestion de la sécurité d'au moins un système informatique présentant une certaine configuration, ledit système informatique étant susceptible d'être affecté par une ou plusieurs vulnérabilités, comportant les étapes :

- De saisie, dans une première base de données (30), de la configuration du système informatique;
- D'établissement d'une seconde base de données (80) regroupant des différentes vulnérabilités connues;
- D'analyse comparative, entre les première et seconde bases de données (30, 80), afin de recenser les vulnérabilités susceptibles d'affecter le système informatique.



FR 2 819 322 - A1



PROCEDE ET DISPOSITIF D'EVALUATION DE LA SECURITE
D'UN SYSTEME INFORMATIQUE

- 5 La présente invention concerne un procédé ainsi qu'un dispositif destinés à évaluer la sécurité d'un système informatique.

On entend par système informatique, un ordinateur ou un ensemble de moyens informatiques comportant une pluralité d'ordinateurs fonctionnant
10 en tant que serveurs ou postes clients, éventuellement reliés entre eux en réseau. Ledit système informatique peut également être éventuellement connecté au réseau mondial connu sous le nom d'Internet.

La cohabitation d'une multitude d'applications logicielles, de systèmes
15 d'exploitation ou encore de protocoles de communications, génère un certain nombre de vulnérabilités auxquelles sont soumis tous les systèmes informatiques. De plus la possible ouverture sur l'extérieur que constitue une connexion au réseau mondial Internet multiplie et amplifie les risques encourus par les systèmes informatiques.

20 Qu'il s'agisse de risques d'intrusion ou encore de problèmes de configuration, la sécurité des systèmes informatiques est mise à l'épreuve à chaque instant. Il est vital, pour tout exploitant d'un système informatique, de pouvoir s'assurer de la sécurité des données stockées,
25 afin de mieux appréhender tout risque de vol, de perte, de destruction ou de détournement de ces données, ou encore de se prémunir contre une consultation ou une modification non autorisée des données.

On connaît certains procédés et/ou dispositifs permettant de sécuriser des
30 systèmes informatiques du point de vue de certaines vulnérabilités, mais

ceux-ci ne peuvent prévoir une protection durable dans le temps compte tenu de la constante apparition de vulnérabilités nouvelles.

5 Ces procédés et/ou dispositifs effectuent des tests périodiques des systèmes informatiques et ne sont donc pas réactifs à l'apparition d'une nouvelle vulnérabilité où lors d'une modification de la configuration des dits systèmes informatiques.

10 D'autres procédés ou dispositifs connus n'ont qu'une action curative ou agissent a posteriori pour bloquer une intrusion mais ne permettent pas de prévoir les différents risques auxquels est exposé un système informatique afin d'exercer une action préventive complète.

15 D'une manière générale, les procédés et/ou dispositifs connus mettent en œuvre des techniques de tests réels des systèmes informatiques à évaluer. Aussi, en cas de test positif d'une vulnérabilité sur un système informatique, des dommages irrémediables peuvent être causés audit système entraînant un arrêt du système ou des pertes de données.

20 Dans ce contexte, la présente invention pallie les inconvénients de l'art antérieur en proposant un procédé ainsi qu'un dispositif permettant d'évaluer de manière permanente et complète les risques encourus par un système informatique, sans avoir recours à des tests sur le système informatique lui-même.

25

A cet effet, selon l'invention, le procédé d'évaluation et de gestion de la sécurité d'au moins un système informatique présentant une certaine configuration, ledit système informatique étant susceptible d'être affecté par une ou plusieurs vulnérabilités, comporte les étapes :

- De saisie, dans une première base de données, de la configuration du système informatique ;
- D'établissement d'une seconde base de données regroupant des différentes vulnérabilités connues ;
- 5 - D'analyse comparative, entre les première et seconde bases de données, afin de recenser les vulnérabilités susceptibles d'affecter le système informatique.

Avantageusement, la seconde base de données recense les conditions
10 d'apparition des différentes vulnérabilités, l'étape d'analyse comparative comportant une étape d'analyse de la présence, dans la configuration du système informatique, de ces conditions d'apparition des vulnérabilités.

En outre, le procédé prévoit une étape d'établissement d'un rapport
15 identifiant les différentes vulnérabilités susceptibles d'affecter le système informatique.

L'invention concerne également un dispositif d'évaluation et de gestion de la sécurité d'au moins un système informatique présentant une certaine
20 configuration, ledit système informatique étant susceptible d'être affecté par une ou plusieurs vulnérabilités, comportant :

- Des moyens de saisie, dans une première base de données, de la configuration du système informatique ;
- Des moyens d'établissement d'une seconde base de données
25 regroupant des différentes vulnérabilités connues ;
- Des moyens d'analyse comparative, entre les première et seconde bases de données, afin de recenser les vulnérabilités susceptibles d'affecter le système informatique.

De préférence, les moyens de saisie de la configuration du système informatique comporte une interface informatique.

5 Selon une forme de réalisation, la seconde base de données recense les conditions d'apparition des différentes vulnérabilités, les moyens d'analyse comparative comportant des moyens d'analyse de la présence, dans la configuration du système informatique, de ces conditions d'apparition des vulnérabilités

10 De manière avantageuse, le dispositif comporte des moyens d'établissement de rapports identifiant les différentes vulnérabilités susceptibles d'affecter le système informatique.

15 Selon une forme préférée de réalisation, les moyens d'analyse comparative comportent un programme d'ordinateur.

L'invention sera mieux comprise à la lumière de la description qui suit, se rapportant à un mode de réalisation illustratif et en aucun cas limitatif en référence aux dessins annexés dans lequel la figure 1 est un diagramme
20 schématique illustrant le procédé selon l'invention.

Dans toute la description qui suit, on entend par système informatique une pluralité d'ordinateurs reliés entre eux à l'aide d'un réseau informatique, éventuellement connectés au réseau mondial Internet.

25 Ainsi, le système informatique présente une configuration générale et chaque ordinateur, qu'il soit serveur ou poste client, dispose d'une configuration propre.

30 Cette configuration propre est composée :

- des caractéristiques propres à l'ordinateur : système d'exploitation, différentes applications fonctionnant sur le poste, périphériques connectés, ...

5

- des différents paramètres de chaque ordinateur, tels que définis, par exemple, dans les fichiers de configuration de chacun d'entre eux.

Par ailleurs, on entend par vulnérabilité tous risques auxquels est susceptible d'être soumis le système informatique, que ce soit l'ensemble des postes reliés en réseau ou un poste précis.

Ces vulnérabilités peuvent être de différents types (risques d'intrusion, perte de données, itérations, etc) et avoir différentes causes (problèmes de paramétrage, de programmation, d'interaction entre des modules incompatibles, problèmes de structuration...).

Ces vulnérabilités peuvent également être classées selon les possibilités d'accès. Certaines vulnérabilités ne peuvent en effet être exploitées qu'avec un accès physique au système informatique, tandis que d'autres peuvent être exploitées à distance.

Enfin, chaque vulnérabilité implique une ou plusieurs conséquences sur chaque ordinateur et/ou sur le système informatique. Ces conséquences peuvent être du type déni de service (partiel ou global), possibilité d'intrusion, avec ce que cela implique en terme de vols, destructions ou modifications de données.

La figure 1 est une représentation schématique du procédé selon l'invention destinée à évaluer la sécurité d'un système informatique.

L'opérateur, mettant en œuvre le procédé selon l'invention, établit un inventaire de la configuration du système informatique à évaluer en répertoriant des informations 10 comportant les caractéristiques principales ainsi que les différents paramètres dudit système informatique, 5 poste par poste par exemple.

Ces informations 10, une fois recensées, sont saisies (étape 20) à l'aide d'une interface graphique, destinée à cet effet, pour être entrées dans une 10 base de données 30.

L'interface graphique présente différents champs permettant de saisir les configurations de chacun des postes.

15 De manière avantageuse, pour des questions de convivialité, chaque champ peut proposer un certain nombre de choix parmi des possibilités recensés dans la base de données 30, sans pour autant limiter les saisies aux choix proposés dans les champs.

20 A titre d'exemple, les différents systèmes d'exploitation connus peuvent être répertoriés dans la base de données 30, et, lorsque l'opérateur doit renseigner le champ « système d'exploitation » de la configuration du poste à évaluer, différentes possibilités lui sont proposées. Cependant, l'opérateur peut également saisir un système d'exploitation qui ne lui est 25 pas proposé.

Selon l'invention, l'interface de saisie des configurations comporte également une partie dont les champs de saisie sont en langage quasi-naturel, et à format beaucoup moins limité que ceux permettant de saisir

les caractéristiques structurelles du poste ou du système informatique à évaluer.

5 Ces champs de saisie permettent à l'opérateur de saisir, par exemple, des préférences en terme de politique de sécurité ou encore des décisions concernant le paramétrage des fichiers de configuration.

10 Par ailleurs, les différentes vulnérabilités connues et telles que définies ci-dessus sont recensées (étape 70) dans une seconde base de données 80.

15 Les vulnérabilités sont ainsi répertoriées en prenant en compte leur type, les causes provoquant leur apparition, ou encore les conséquences qu'elles sont susceptibles d'engendrer sur le système informatique.

Le recensement des différentes vulnérabilités peut avantageusement être le résultat de la conjugaison de travaux de recherche et de développement et d'une veille technologique systématique.

20 Ainsi, les travaux de recherche et de développement lui permettent d'obtenir un premier lot d'informations 50 sur les vulnérabilités tandis que la veille technologique lui fournit un second lot d'informations 60 complémentaires du premier lot 50.

25 Ces lots d'informations (50, 60) permettent à l'opérateur de regrouper les différents types de vulnérabilité ainsi que leurs caractéristiques dans la seconde base de données 80.

30 Ce regroupement dans la seconde base de données 80 est effectué au moyen d'une interface de saisie (étape 70) comportant un certain nombre

de champs destinés à entrer les informations provenant des premiers et seconds lots d'informations (50, 60).

5 Cette modélisation des vulnérabilités permet notamment de recenser, dans la seconde base 80, l'ensemble des conditions devant être réunies pour qu'apparaisse une vulnérabilité. Ces conditions sont d'ordre structurel, c'est-à-dire dépendant à la fois du type de matériel composant le système informatique, des logiciels installés ainsi que des versions desdits logiciels, etc.

10

Chaque vulnérabilité est également modélisée de manière à recenser l'ensemble des modifications d'une configuration donnée susceptibles de faire apparaître la vulnérabilité.

15 Une fois les configurations et les vulnérabilités saisies lors des étapes 20 et 70, une analyse comparative entre la première base de données 30 et la seconde base de données 80 est effectuée à l'aide d'un moteur d'analyse 40 réalisé par l'intermédiaire d'un programme d'ordinateur.

20 Ce moteur d'analyse 40 effectue, de manière connue, une série d'allers et retours entre la première base de données 30 et la seconde base de données 80 afin d'identifier, parmi les différentes vulnérabilités recensées dans la seconde base de données 80, celles qui sont susceptibles d'affecter le système informatique dont la configuration est recensée dans
25 la première base de données 30.

Le moteur d'analyse effectue ainsi une analyse de la présence, dans la configuration du système informatique, de ces conditions d'apparition des vulnérabilités répertoriées dans la seconde base de données 80.

Après un nombre minimum d'aller-retour entre les deux bases de données (30, 80) le moteur d'analyse 40 est en mesure de déterminer, parmi les vulnérabilités recensées dans la seconde base de données 80, lesquelles sont susceptibles d'affecter un système informatique particulier dont la configuration a été saisie et modélisée dans la première base de données 30.

Dans le cas où une configuration présente presque toutes les conditions d'apparition d'une vulnérabilité particulière, le moteur d'analyse 40 peut, par l'intermédiaire d'un rapport tel que décrit plus loin, attirer l'attention de l'opérateur sur les conditions manquantes afin que ce dernier vérifie si ces conditions manquantes sont présentes au niveau du système informatique et n'auraient pas été saisies car secondaires. L'opérateur complète alors éventuellement la configuration saisie dans la première base de données 30 qui est ainsi affinée et tend de plus en plus vers la configuration réelle du système informatique.

Selon l'utilisation du système informatique et/ou le type de vulnérabilité, un niveau de sécurité peut être déterminé et, en conséquence, le moteur d'analyse 40 évalue le danger potentiel que représentent les différentes vulnérabilités détectées.

Il est entendu que la première base de données 30 peut recenser les configurations d'une multitude de postes ou de systèmes informatiques dont la sécurité sera évaluée selon le procédé décrit ci-dessus.

Le dispositif selon l'invention comporte en outre, des moyens d'établissement de rapports, connus en eux-mêmes, permettant de délivrer les résultats de l'analyse comparative pour chacun des systèmes informatiques recensés dans la première base de données 30.

Chaque rapport 90 peut avantageusement contenir :

- 5 - le nombre de vulnérabilités susceptibles d'affecter le système informatique ;
- le risque que représente chaque type de vulnérabilité ;
- une description de chaque vulnérabilité détaillant le type, la cause, la portée ainsi que les conséquences engendrées par une telle vulnérabilité ;

10

Cette liste n'est pas limitative et peut contenir tous types d'informations susceptibles d'évaluer la sécurité de chaque poste ou du système informatique général, en particulier les points faibles d'un système informatique.

15

Le rapport 90 peut lister les postes où une intrusion serait relativement aisée et connectés à d'autres postes comportant des données sensibles, et présentant eux une protection efficace. En effet, certains postes sensibles non sujets à certaines vulnérabilités peuvent être connectés à
20 d'autres postes qui présentent des faiblesses et un intrus pourrait accéder aux postes sensibles en passant par les postes moins protégés. L'invention permet, par l'intermédiaire notamment des rapports 90, de connaître à tous moments les points faibles d'un système informatique.

25 Ces rapports 90 d'évaluation de la sécurité peuvent être sous format papier ou, avantageusement, électronique afin d'être immédiatement disponible pour le titulaire du système informatique évalué.

Le procédé selon la présente invention présente l'avantage de ne réaliser
30 aucun test réel sur chaque poste ou sur le système informatique général.

En effet, il s'agit de simulation et non de test, ce qui permet d'évaluer la sécurité d'un système très en aval, dès la découverte d'une vulnérabilité et donc bien avant qu'elle ne soit exploitée par quelqu'un.

5

Ainsi, dès qu'une nouvelle vulnérabilité est découverte par l'intermédiaire (recherche et développement ou veille technologique), cette nouvelle vulnérabilité est incorporée à la seconde base de données 80 et le moteur d'analyse 40 permet de déceler tous les systèmes informatiques recensés
10 dans la première base de données 30 susceptibles d'être affectés par cette nouvelle vulnérabilité.

Le procédé et le dispositif selon l'invention permettent donc d'avertir le titulaire d'un système informatique potentiellement fragilisé au plus tôt, et
15 de prendre les mesures adéquates afin de se prémunir contre la nouvelle vulnérabilité.

En outre, en cas de modification d'une configuration d'un système informatique recensée dans la première base de données 30, le moteur
20 d'analyse 40 permet de déceler immédiatement les vulnérabilités susceptibles d'affecter la nouvelle configuration du système informatique.

Ainsi, le procédé et le dispositif selon l'invention permettent d'étudier l'impact d'une modification de configuration future sans avoir à effectuer
25 cette modification.

Que ce soit à base de configuration 30 constante avec une évolution de la base de vulnérabilité 80, ou à base de vulnérabilité 80 constante avec une évolution de la base de configuration 30, ou encore lorsque les deux
30 bases 30 et 80 sont en évolution, le procédé selon la présente invention

permet de déceler à tout instant tous types de vulnérabilités susceptibles d'affecter un système informatique recensé dans la première base 30.

Avantageusement, les moyens d'établissement de rapports peuvent également éditer des rapports 100 recensant les actions à ne pas
5 entreprendre sous peine de voir un système informatique recensé dans la première base de donnée 30 être affecté par une vulnérabilité recensée dans la seconde base 80.

10 Par exemple, le rapport 100 peut mettre en avant les modifications de configuration à ne pas effectuer sous peine de voir apparaître la vulnérabilité, comme l'utilisation d'un nouveau protocole, l'installation d'un certain logiciel, etc.

15 Ainsi, le procédé et le dispositif selon l'invention permettent de connaître en temps réel la vulnérabilité d'un système informatique, l'impact d'une modification envisagée dans la configuration dudit système informatique, tout en pouvant définir le niveau de sécurité souhaité, et ce avant qu'une quelconque vulnérabilité ne vienne affecter le système informatique.

20

L'évaluation selon l'invention est effectuée par simulation, les différents paramètres de ladite simulation (paramètres de la configuration du ou des systèmes informatiques ou des vulnérabilités recensées) étant à tout instant aptes à être modifiés afin de correspondre au mieux à la situation
25 réelle envisagée.

REVENDICATIONS

- 5 1. Procédé d'évaluation et de gestion de la sécurité d'au moins un système informatique présentant une certaine configuration, ledit système informatique étant susceptible d'être affecté par une ou plusieurs vulnérabilités, comportant les étapes :
- De saisie, dans une première base de données (30), de la
10 configuration du système informatique ;
 - D'établissement d'une seconde base de données (80) regroupant des différentes vulnérabilités connues ;
 - D'analyse comparative, entre les première et seconde bases de données (30, 80), afin de recenser les vulnérabilités susceptibles
15 d'affecter le système informatique.
- 20 2. Procédé selon la revendication 1, caractérisé en ce que la seconde base de données (80) recense les conditions d'apparition des différentes vulnérabilités, l'étape d'analyse comparative comportant une étape d'analyse de la présence, dans la configuration du système informatique, de ces conditions d'apparition des vulnérabilités.
- 25 3. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte, en outre, une étape d'établissement d'un rapport (90) identifiant les différentes vulnérabilités susceptibles d'affecter le système informatique.
4. Dispositif d'évaluation et de gestion de la sécurité d'au moins un système informatique présentant une certaine configuration, ledit

système informatique étant susceptible d'être affecté par une ou plusieurs vulnérabilités, comportant :

- Des moyens de saisie, dans une première base de données (30), de la configuration du système informatique ;
- 5 - Des moyens d'établissement d'une seconde base de données (80) regroupant des différentes vulnérabilités connues ;
- Des moyens d'analyse comparative (40), entre les première et seconde bases de données (30, 80), afin de recenser les vulnérabilités susceptibles d'affecter le système informatique.

10

5. Dispositif selon la revendication 4, caractérisé en ce que les moyens de saisie de la configuration du système informatique comporte une interface informatique.

15 6. Dispositif selon l'une des revendications 4 ou 5, caractérisé en ce que la seconde base de données (80) recense les conditions d'apparition des différentes vulnérabilités, les moyens d'analyse comparative (40) comportant des moyens d'analyse de la présence, dans la configuration du système informatique, de ces conditions d'apparition
20 des vulnérabilités.

7. Dispositif selon l'une des revendications 4 à 6, caractérisé en ce qu'il comporte, en outre, des moyens d'établissement d'un rapport (90) identifiant les différentes vulnérabilités susceptibles d'affecter le
25 système informatique.

8. Dispositif selon l'une des revendications 4 à 7, caractérisé en ce que les moyens d'analyse comparative (40) comportent un programme d'ordinateur.

30

1/1

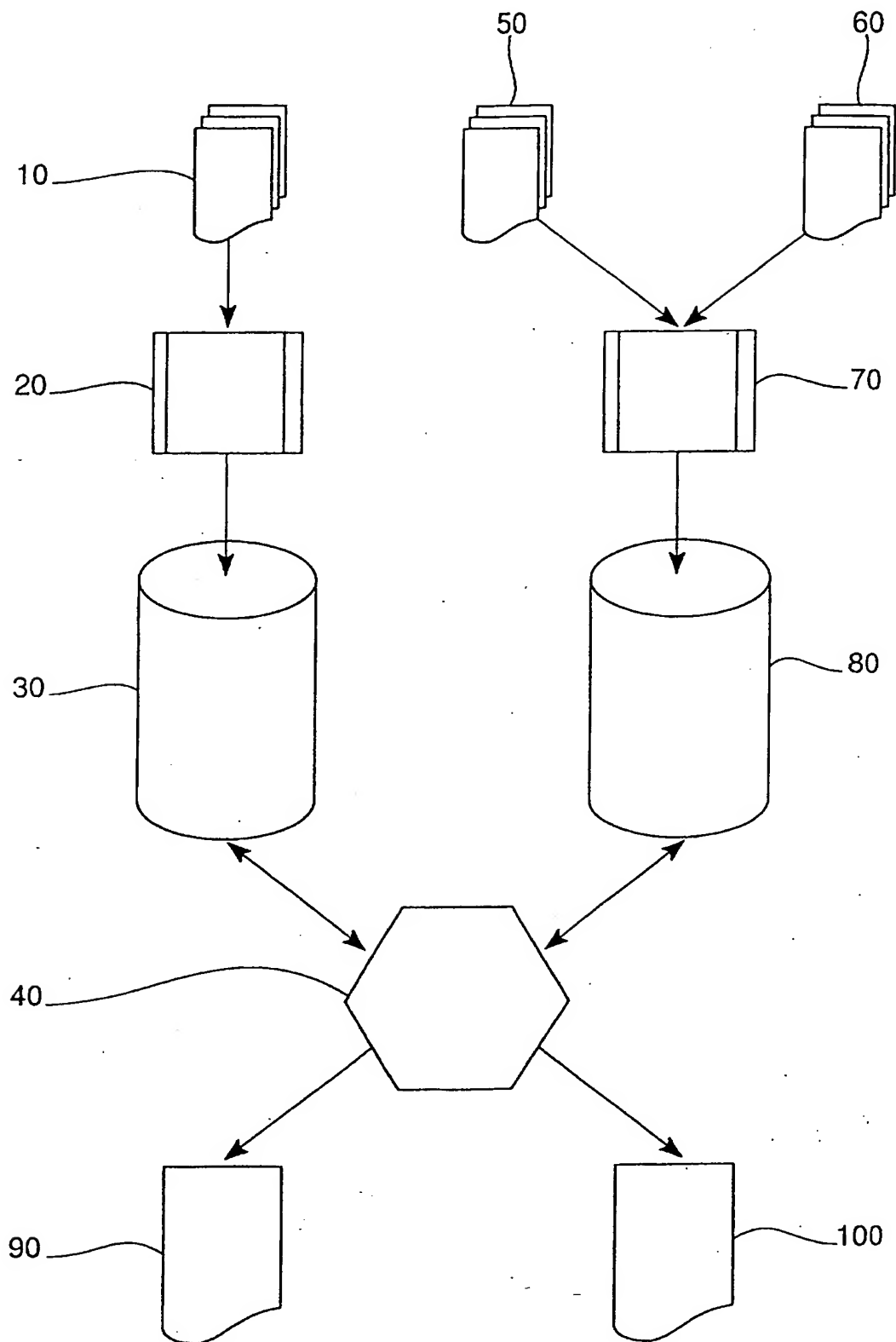


FIG. 1

2819322

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE**RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0100192 FA 597094**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 27-09-2001

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0070463 A	23-11-2000	AU 4833300 A	05-12-2000
		AU 4833400 A	05-12-2000
		WO 0070463 A1	23-11-2000
		WO 0070464 A1	23-11-2000
US 5485409 A	16-01-1996	AUCUN	
US 5850516 A	15-12-1998	AUCUN	
US 5819226 A	06-10-1998	AU 4850093 A	29-03-1994
		CA 2144068 A1	17-03-1994
		DE 69315356 D1	02-01-1998
		DE 69315356 T2	18-06-1998
		EP 0669032 A1	30-08-1995
		ES 2108880 T3	01-01-1998
		JP 8504284 T	07-05-1996
		WO 9406103 A1	17-03-1994

EPO FORM P0485

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82